Remarks

The applicants have carefully reviewed the Advisory Action dated October 10, 2007, the final Office action dated July 30, 2007, and the art applied therein to the claims. Claims 1-11, 13, 16, and 18-29 are pending and at issue, claims 1, 6, 7, 10, 11, 16, 18, 19, 22-24, and 26 are amended, claims 12, 14, 15, and 17 are cancelled, and claims 27-29 are added for consideration, of which claims 1, 10, 18, and 25 are independent. No new matter has been added. In view of the foregoing amendments and the following remarks, reconsideration and allowance of the application are respectfully requested.

As a preliminary matter, the applicants identify that claims 11, 16, 19, 22-24, and 26 are amended because of, in part, an erroneous listing of claim dependency that occurred in the prior response to the Office action dated January 31, 2007. However, amendments with respect to claim dependency for claims 11, 16, 19, 22-24, and 26 now reflect proper claim dependency.

The Rejections Under 35 U.S.C. §102(e)

In the Office action, claims 1, 5-10, 14-18, and 22-26 were rejected as anticipated by Griffin et al. (U.S. Patent No. 7,076,655 – hereinafter "Griffin"). As explained below, the applicants respectfully submit that independent claims 1, 10, 18, and 25, and all claims dependent therefrom, are allowable over the art of record.

Independent claims 1, 10, and 18 recite, *inter alia*, determining if a user credential is authorized to allow booting of a desired operating system, and enabling booting of the

desired operating system if the user credential is authorized to allow booting of the desired operating system.

It is well settled that "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 2 USPQ2d 1051 (Fed. Cir. 1987) (emphasis added). As explained below, the applicants submit that Griffin fails to describe or suggest determining if a user credential is authorized to allow booting of a desired operating system, and enabling booting of the desired operating system if the user credential is authorized to allow booting of the desired operating system, as recited in claim 1, 10, and 18.

Griffin describes a host computing platform in which multiple computing environments may execute. *Griffin*, 1:32-35. Of particular concern is verification that each of the multiple computing environments are separate, logically distinct, and independently trustworthy. *Griffin*, 1:37-40. To facilitate such verification, Griffin describes that each computing environment employs an identity label that may be supplied to a challenger (e.g., a user) prior to that challenger issuing an identity challenge. *Griffin*, 2:3-8. In other words, Griffin provides a method for a user to verify that a particular computing environment is what it purports to be, thereby minimizing and/or eliminating the possibility of the user being exposed to a subverted computing environment. *Griffin*, 1:48-50.

While Griffin describes using a secure channel between a user and a computing platform that accommodates any suitable authentication technique(s), Griffin fails to describe or suggest any manner of discriminating access to the user. *Griffin*, 5:51-62. In

fact, Griffin describes that a computing platform provides a plurality of discrete computing environments without regard to authorized credentials, much less determining if the user credential is authorized to allow booting of a desired operating system. Any authentication of the user occurs for the benefit of such user obtaining an opportunity to issue an integrity challenge (*Griffin*, 10:3-13) rather than any such authorization to dictate operating system booting authorization. At best, Griffin describes a restriction of one or more processes within a compartment that could have an effect on network access or access to files outside of the compartment (*Griffin*, 6:4-12), but Griffin is completely silent to an operating system to be booted, determining if a user credential is authorized to allow booting of the desired operating system, and enabling booting of the desired operating system if the user credential is authorized to allow booting of the desired operating system, as recited in claims 1, 10, and 18.

Unlike restricting a user, much less determining if a user credential is authorized to allow booting of a desired operating system, Griffin describes restriction of processes (*Griffin*, 7:36-38) and employs a virtual machine to protect a host operating system from access by a process (*Griffin*, 7:41-44). To that end, Griffin may ensure that a process is limited to computing platform resources having an appropriate degree (Griffin, 7:48-52), but Griffin does not address user limitation(s), user credentials associated with a desired operating system to be booted, or determining if the user credential is authorized to allow booting of the desired operating system. Moreover, in the event that the user credential is authorized to allow booting of the desired operating system, Griffin fails to describe or suggest enabling booting of the desired operating system in response thereto.

As a result, because Griffin fails to describe or suggest determining if a user credential is authorized to allow booting of a desired operating system, and enabling booting of the desired operating system if the user credential is authorized to allow booting of the desired operating system, Griffin cannot anticipate claims 1, 10, and 18. To that end, the applicants respectfully request that the rejection of claims 1, 10, and 18, and all claims dependent therefrom, be withdrawn for at least these reasons.

Independent claim 25 recites, *inter alia*, a permissions table storing user credentials and boot objects corresponding to the user credentials, and a user verification segment determining if the submitted user credential is authorized to boot a desired operating system.

The examiner appears to assert that the platform configuration registers (PCRs) of Griffin shown in FIG. 3 suffice as teaching a permissions table and/or user credentials and boot objects. However, unlike user credentials, Griffin describes the trusted device is arranged to form an integrity metric of the host operating system. The trusted device of FIG. 3 cannot be fairly construed as a permissions table storing user credentials, particularly in view of Griffin's teaching that each PCR stores a hash value representing an integrity metric, which is information concerning the integrity of each computing environment, not a user. *Griffin*, 8:34-46. Furthermore, Griffin is completely silent regarding whether such PCRs include boot objects, much less a permissions table storing user credentials and boot objects corresponding to the user credentials, as recited in claim 25.

The examiner also appears to assert that mere user establishment of a secure channel via signature authentication constitutes a user verification segment determining if

the submitted user credential is authorized to boot a desired operating system. However, while Griffin describes employing trusted hardware with, for example, a smart card, such authorization fails to address operating system selection, much less authorization to boot a desired operating system. As described above, the authorization by Griffin merely allows the user to request demonstration of the integrity of a computing environment by, initially, establishing a secure channel to the trusted device, but Griffin fails to describe or suggest a user verification segment determining if the submitted user credential is authorized to boot a desired operating system, as recited in claim 25.

As a result, because Griffin fails to describe or suggest a permissions table storing user credentials and boot objects corresponding to the user credentials, and a user verification segment determining if the submitted user credential is authorized to boot a desired operating system, Griffin cannot anticipate claim 25. To that end, the applicants respectfully request that the rejection of claim 25, and corresponding dependent claim 26, be withdrawn for at least these reasons.

The applicants also submit that dependent claims 27-29 are allowable over the art of record. In particular, claims 27-29 depend from claims 1, 10, and 18, respectively, each of which are independent claims believed to be allowable over the art of record. No new matter has been added.

Conclusion

The applicants respectfully submit that all claims are in condition for allowance. Reconsideration of the application and allowance thereof are respectfully requested. If

there is any matter that the examiner would like to discuss, the examiner is invited to contact the undersigned representative at the telephone number set forth below.

Respectfully submitted,

HANLEY, FLIGHT & ZIMMERMAN, LLC
150 South Wacker Drive
Suite 2100
Chicago, Illinois 60606
(312) 580-1020

By: **/Peter J. Cesarz /**
Peter J. Cesarz
Registration No. 61,190
Agent for the Applicants

Dated: October 30, 2007